# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

## OVERVIEW OF HACKING TOOLS AND PROTECTION OF MODERN ICT DEVICES.

*P.A. Kabanov, M.S. Sukhodoev*
*(Tomsk, Tomsk Polytechnik University)*
*E-mail: Peter96pvl@gmail.com, smike@tpu.ru*

**Abstract** — this article describes security threats possibility in modern devices, and also teaches how to properly protect yourself and your confidential information.

**Keywords** — information security, InfoSec, hacking tools, modern ICT devices, programming, vulnerabilities.

**Introduction.** The question of protecting the information of each user on the network is becoming more relevant. An attacker, if he is one, can use confidential information for various purposes: blackmail, extortion, and sale. Ultimately, it can be used to obtain some benefit that the attacker is pursuing. A user's computer that is connected to the network may be a subject to virus attacks at any time. Antivirus programs protect computer, but not fully. The situation is getting worth by exploring of new ways of penetration, which can cause deplorable consequences – a burned-out fee, debited money from a bank account, and disclosure of confidential information. This paper describes the various possibilities of hacking and taking precautions to avoid negative consequences.

**Kali Linux and its features.** For a successful attack, you may need a long preparation, study and a long process of hacking, and importantly – hiding your PC [1].

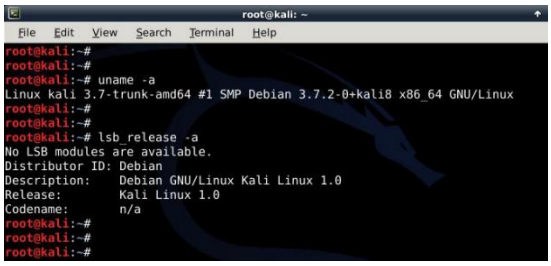


**Fig. 1.The Kali Linux Terminal**

Kali Linux is the GNU / Linux-LiveCD, which has appeared from the WHAX and Auditor Security Collection union. This operating system was created specifically for testing protection, finding backdoors and eliminating them. Both information security specialists and professional hackers may use it, because it has a wide range software for various needs. So why Linux and not Windows? Linux is a more flexible system. You can control the Linux system core and all the functionality through the console (see Figure 1). Many people avoid this system, although it is easy to learn. The Windows OS is needed for comfort and performance, but far from being suitable for hacking because managing the kernel is not so easy. Anonymity is a very important part, and in Windows, it is easy to read the action history. It is also very easy to connect portable media with a live version of the Kali Linux to any computer with a network access and get started.

Let us get straight to the point. We know that there are the following types of encryption: WEP, WPS, WPA, WPA 2 PSK / ENTERPRISE. The most common are the last two types of encryption. First we run the terminal, check the available network interfaces using the "iwconfig" command (see Figure 2).


**Fig. 2. An overview of the "iwconfig" command**

For further action, we will need the installed airplay-ng utility (mostly preinstalled in the Kali Linux). We select the interface and translate the network card into the monitoring mode, having previously closed all the commands that interfere with our interface using the kill command. In our example, we use wlan1. We register the “airmon-ng start wlan1” command (see Figure 3). The interface will change its name to “wlan1mon” and will go into the network-monitoring mode.

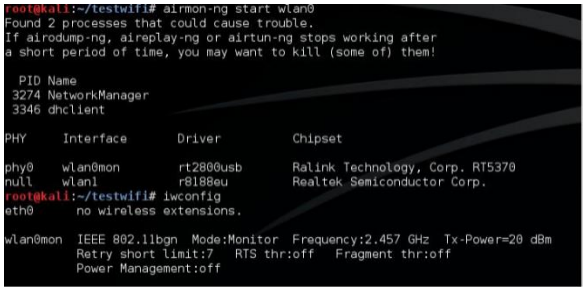


**Fig. 3. An overview of the "airmon-ng" tool**

Next, we display a complete list of available access points and their information (see Figure 4) using “airodump-ng wlan1mon” command. When selecting a particular point, we switch only to its monitoring. In our example, we do this with the following command: “airodump-ng wlan0mon --bssid FC:8B:97:57:97:A9 --channel 2 --write handshake –wps” (wps is indicated as an alternative – if the device does not have a better protection).


**Fig. 4. Complete list of available access points and their information**

Explanation of the figure: BSSID – is the mac-address of the access point, PWR – is the signal strength (that is measured in the negative range), CH ¬– is the connection channel, ENC – is the encryption type, ESSID – is the network name, STATION – is the mac-address of the connected device, Frames – is the number of transmitted frames. We monitor the network with the mac-address FC:8B:97:57:97:A9 on the second channel, we also take into account the presence of WPS encryption of this network.

Then we should force the user to connect to the network again. For this, a DE-authentication attack will be used – it allows transmitting corrupted packets to the access point, which will force it to restart. An example of the command is “aireplay-ng -0 10 –a FC:8B:97:57:97:A9 –c 68:3E:34:15:39:9E wlan0mon”. Explanation: -0 – is the DE-authentication procedure, 10 – is a number of repetitions, –a – is the mac-address of the point, -c – is the address of the client. Next, we take a closer look at this type of attack. After we intercept the handshake, we should save the .pcap session to proceed to the next stage.

The last and possibly the most difficult stage is a brute force or a dictionary searching for getting a password [2]. For this, we use the built-in brute “aircrack-ng” command. It is necessary to negotiate that the password will be searched using our CPU or GPU and it can take much time to search for it. It is always possible to customize the “brute force” algorithm, at will. We also may need to make an approximate dictionary of passwords, or you have to go through everything character by character. The more information we have about the password itself (which characters are exactly used, the length of the password, the place of the character in the password), the faster we can find it. After the search, the password will be displayed, and we will get into the network (see Figure 5).

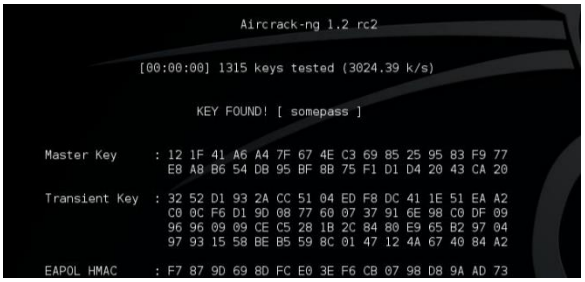


**Fig. 5. Result of “brute force”**

Question? In addition, why does the attacker hack Wi-Fi and how can he use it? It is simple – when an attacker enters the network, he can fully analyze the traffic. That is, he can know when, to whom and even what you sent, your social network accounts and much more, there is already a matter of intent. How to protect yourself? Set long and complex passwords for the access point, as well as periodically change them. Also, try to avoid WPS level protection and use modern encryptions.

**Vulnerabilities of Wi-Fi networks, routers and their hacking.** However, that is not all. There are workarounds such as- hacking the router. For this, we will use the program “hydra” (see Figure 6). The hydra program supports a huge number of services. Due to its speed and reliability, it has earned a well-deserved mark among penetration testers. Usually, after installing a Wi-Fi router, few people change standard logins and passwords. Mostly they are admin / admin, root / admin, admin / 0000 and so on [3]. For such purposes, naturally, no third-party applications like “hydra” are needed. It is enough to know the standard logins and passwords for certain models of the router, then manually enter them, after which we will find yourself in the administration panel, where you can either completely break the router or change the access point password. Using this panel, we can enter the network, or just find out all the necessary information. Of course, now we will consider the option when the login and password are non-standard.

The Kali Linux has “hydra” utility already installed, so let us get to the command overview. As in the previous example, we will need a dictionary of possible logins and passwords, or we will have to do a complete search. We can find the most popular logins and passwords throught the Internet. The hydra utility is a multifunctional program and can be represented for a very long time, so we consider the case when we have a dictionary with logins and passwords (logins.txt, passwords.txt). Then the command will look like this: “hydra -L logins.txt -P passwords.txt –s 80 192.168.0.1 http-get /”. Explanation: –L – the usage of a login file, -P ¬– the usage of a password file, -s ¬– is the port on which the attack is made.

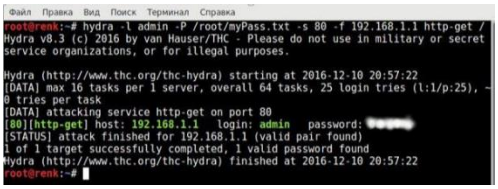


**Fig. 6. An overview of the "hydra" tool**

How to protect yourself from hacking a router? Never leave the login and password in the factory state (by default), and generate it for your own.

**Analysis of network traffic and search for relevant information.** Now we go directly to the analysis of traffic and network information. By itself, the analysis of traffic is called sniffing, and the program that analyses it – sniffers [6]. The most famous sniffer program is the Wireshark.

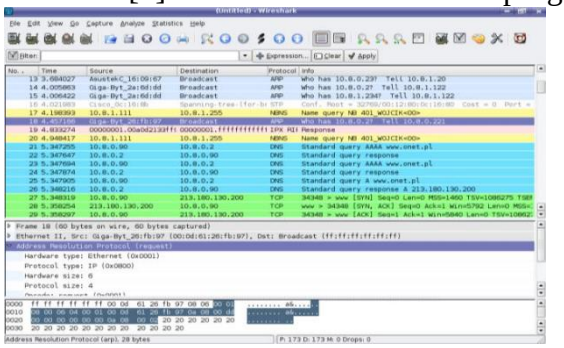

**Fig. 7. An overview of the "Wireshark" tool**

In Kali Linux, in addition to Wireshark, a “tcpdump” (see Figure 8) utility is available on UNIX systems.

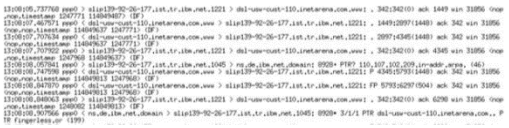

**Fig. 8. An example of the ”tcpdump” tool output**

The advantage of Wireshark is the presence of a graphical interface, simpler use and filtering and sorting capabilities. An example for comparing what the Wireshark and the tcpdump looks like, it will be easier for a beginner to get comfortable with the first option. The Wireshark is also cross-platform tool, so it can be used on various operating systems. With the help of sniffers, you can intercept the logins and passwords of network users; find out the information they send; intercept confidential photo / video / messages.

How to protect yourself? Use https connections, encryption, and check your network card for the ability to work in “promiscuous mode” (random mode of receiving and transmitting all packets).

**DOS, DDOS, DE-authentication attacks, network spam.** Now consider about a denial of service attack or DOS attack. When we were hacking a Wi-Fi router, we used such a type of an attack, which was called a deauthentication attack. The difference between our attack is that it sent only 10 corrupted packets, and only for a specific user. With a DOS attack, we would send an uncontrolled number of packets to the access point for all connected users, until this access point become turned off. Typically, such attacks are rarely carried out on one person, mainly on the owners of servers, websites and other services, but it is still important to know – you should always be ready and prepared for this type of attack: have a backup server, all servers should be prepared for a remote reboot , the software should be updated and have as few vulnerabilities as possible.

**IP camera vulnerabilities.** Most devices that are connected to the network have vulnerabilities [4]. For example - IP-cameras. Now, most people switched to such surveillance cameras, abandoning the analog. They are easy to use and monitor, but also have their own vulnerabilities. In addition, all the vulnerabilities are reduced to one thing- during installation, standard logins and passwords are specified. It is not difficult to hack such devices. I will show an example.

Task: hack IP-cameras with standard logins and passwords in the city. To begin, we will need to compile a dictionary of standard logins and passwords (again, there are many of them on the

network, especially models, you can add it yourself). Next, you should find out the current IP-range of a region or city (see Figure 9). After that, you can start scanning.

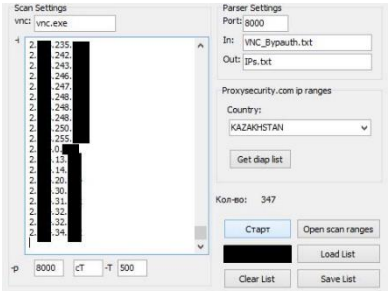


**Fig. 9.Range selection**

If successful, the screenshots with logins and passwords from the camera, as well as the IP-address are saved (see Figure 10).

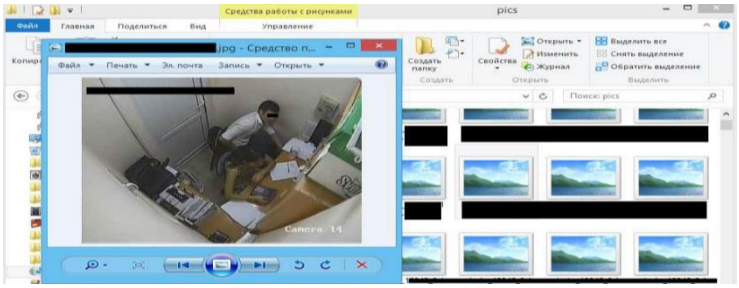

**Fig. 10. Saved screenshots from IP-camera.**

After that, we can connect to them and watch at any time through specialized programs for remote viewing of video cameras. The attacker may use this information for extortion, compromising, trimming crimes, turning off the camera.

How to protect yourself? Again - always put your own logins and passwords do not leave the factory default ones.

**Root the smartphone and use its capabilities.** Many people wonder if it is possible to do the entire above, but with the help of your smartphone. After all, there is not always a computer or a laptop at hand. Yes, much of the above can be done with the help of your smartphone, and if you have a delicate knowledge of writing applications for a smartphone and flashing it, the possibilities increase [5].

The best program for analyzing traffic, data interception, carrying out attacks substitution, SSL-strip, interception cookie is an “intercepter-ng”. To install it, you will need to tinker with the firmware kernel, as well as get root-rights to the smartphone, but it is worth it. I will show with an example of hacking into my student’s personal account (I had my own personal account in it, during the training and all penetration tests were performed during the same training).

First, we check the entire network for connected devices; in this case, it is my laptop, smartphone and access point itself. We choose whom we will monitor and get down to work. To begin with, we set up “Intercepter-ng” to work (see Figure 11). It all depends on what types of attacks we will conduct. In this case, we will steal the cookie session, login and password. After setting required options, we can start work. After some time, the Intercepter-ng tool discovers that I have entered the site, shows my personal account, and immediately intercepts the login, password and cookie session. After that, we can freely see what the user sees, and after his release - log in from his account on his own.


**Fig. 11. An overview of the "Intercepter-ng" tool**

After all, we turn off the utilities and check if we have not been noticed on the network, and whether attacks have been made, (we clean up the tracks) (see Figure 11).

**Conclusion.** It is impossible to be completely protected, and even more so 100% sure of this. The most important rule is to remember the basic principles of information security (and be a little paranoid).

All information has been provided for educational purposes and does not encourage you to use it for criminal purposes. All checks were carried out on their own devices and (or) the permission of their owners.

REFERENCES

1. Georgia Weidman. Penetration Testing: A Hands-On Introduction to Hacking. – M.: No Starch Press, 2014. – 528 с.
2. Thomas Wilhelm. Professional Penetration Testing. – M.: , 2010. – 528 с.
3. Chris Hurley. WarDriving and Wireless Penetration Testing. – M.: , 2010. – 0 с.
4. David Maynor. Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research. – M.: , 2010. – 350 с.
5. Gray Hat Hacking The Ethical Hackers Handbook, 3Rd Edition. – M.: , 2011. – 720 с.
6. Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense (Lecture ... Computer Science / Security and Cryptology). – M.: , 2012. – 371 с.
7. Imran Sohail and Sikandar Hayat. Network Security and DDoS. – M.: LAP Lambert Academic Publishing, 2010. – 64 с.

## MDS-МАТРИЦЫ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

*Т.К. Жукабаева, А.А. Абдилдаева, Е.М. Марденов*
*(Нур-Султан, Казахстан. Институт Информационных и Вычислительных Технологий)*
*tamara_kokenovna@mail.ru, abass_81@mail.ru , uvideooperator@mail.ru*

## MDS MATRICES AND THEIR USE IN CRYPTOGRAPHY

*T.K. Zhukabayeva, A.A. Abdildayeva, E.M. Mardenov*
*(Nur-Sultan, Kazakhstan. Institute of Information and Computing Technologies)*
*tamara_kokenovna@mail.ru, abass_81@mail.ru , uvideooperator@mail.ru*

**Abstract:** In this article, we study the properties of MDS matrices by considering the concepts of a cycle and construct MDS matrices. MDS matrices have an important place in cryptography and can be used